Email Security Update

Technology with Integrity

By Tim Torian, Torian Group, Inc.

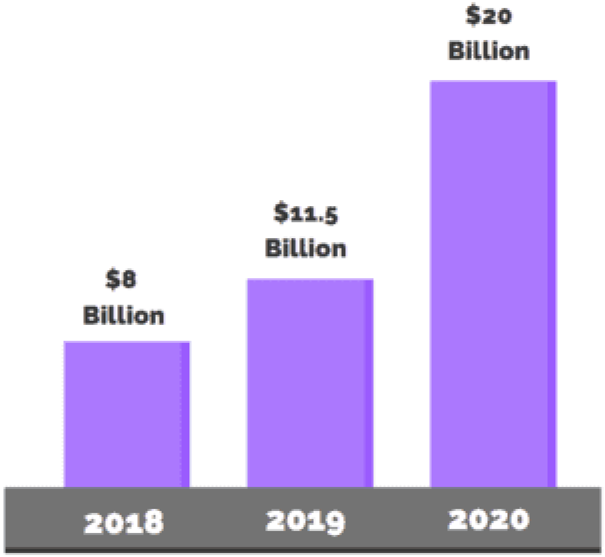
Summary:

Email is essential yet vulnerable to abuse. Use an email program that is backed by adequate security and enable the security features available. Attacks have become more sophisticated. Protect your staff from phishing and malware. Avoid getting your email hacked and abused. Protect your company from attack by implementing recently developed tools.

1. Use Microsoft or Google to host your email.
2. Set up Two-Factor Authentication.
3. Use Outlook where possible. Avoid Webmail.
4. Separate work email.
5. Enable advanced malware and phishing protection in Office 365

The Risk

We have all seen lots of scary statistics. It can be easy to ignore them after a while.



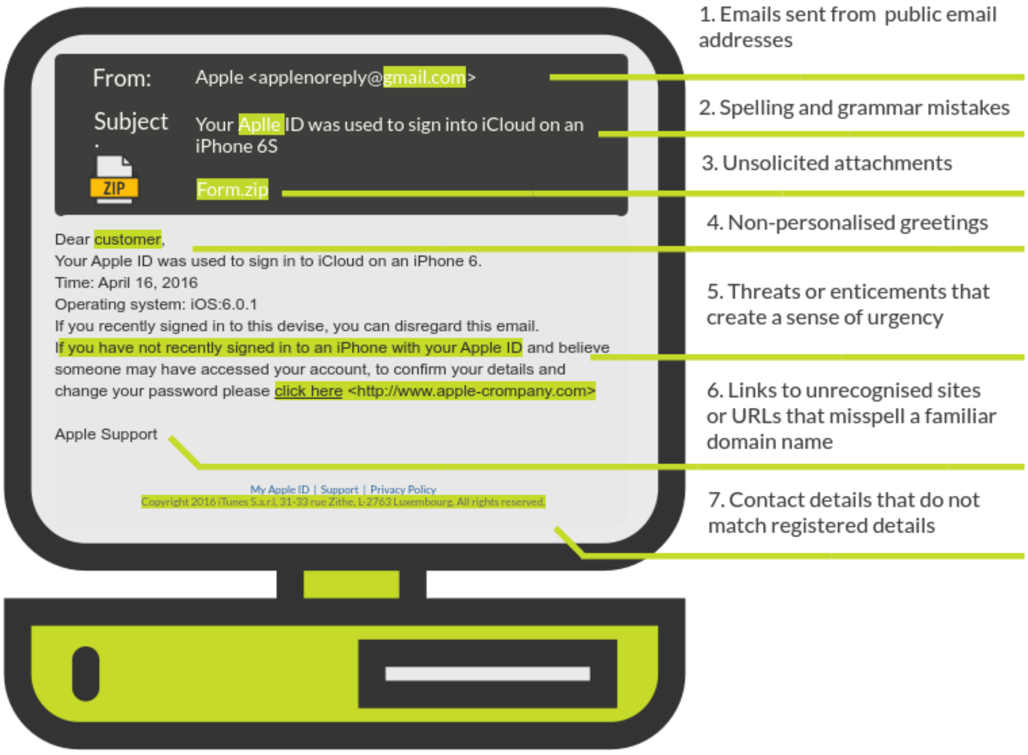
*Estimated global damage from ransomware.

96% of phishing attacks arrive by email.
43% of data breaches involve email. 22% involved phishing.
75% of US organizations have experienced a successful phishing attack.

It is well known that email is a primary target for hackers, and that many email users are likely to click on a link or open a file that delivers malware.

Once someone has access to your email, that person can then impersonate you to compromise others, recover passwords from your banking and credit card sites, and use your email address for additional malware campaigns.

What you knew about detecting phishing has changed. Many malicious emails are extremely well crafted, using an exact copy of a legitimate message with a link that looks credible.



From: Apple <applenoreply@gmail.com>

Subject Your Aplle ID was used to sign into iCloud on an iPhone 6S

ZIP Form.zip

Dear customer,
Your Apple ID was used to sign in to iCloud on an iPhone 6.
Time: April 16, 2016
Operating system: iOS:6.0.1
If you recently signed in to this devise, you can disregard this email.
If you have not recently signed in to an iPhone with your Apple ID and believe someone may have accessed your account, to confirm your details and change your password please click here <http://www.apple-crompany.com>

Apple Support

My Apple ID | Support | Privacy Policy
Copyright 2016 iTunes S.a.r.l, 31-33 rue Zithe, L-2763 Luxembourg. All rights reserved.

1. Emails sent from public email addresses

2. Spelling and grammar mistakes

3. Unsolicited attachments

4. Non-personalised greetings

5. Threats or enticements that create a sense of urgency

6. Links to unrecognised sites or URLs that misspell a familiar domain name

7. Contact details that do not match registered details

[The usual advice can leave your business exposed to phishing](#)

In addition, criminals can gather information about you from social media and public websites to make email look like it is from someone you know or trust.

The Benefits of good security

Cyber-insurance agencies are requiring that insured companies follow basic security practices to prevent ransomware and security breaches. These include protecting your email.

Many companies are required to follow security best practices by law. This includes PCI-DSS requirements for those that process credit cards, IRS requirements and GLBA requirements for CPAs and financial firms, and HIPAA requirements for health practitioners.

And… preventing your company from getting hacked is just good business.

What to do to secure your email

1. **Select an email hosting company that can help protect your email.**

We strongly recommend Microsoft Exchange Online (Microsoft 365). Microsoft is one of the leaders in email security, and it is fully integrated with Outlook.
Gmail for business also does an excellent job of protecting and filtering email.

What you don't want is to host your email with the company that hosts your website or use the email that comes with your internet connection. Their business is not focused on email security, and they don't have the resources to keep up with the changes in phishing and hacking tools. Here is an article which explains this in depth if you need more convincing.

2. **Use Two-Factor Authentication.**

Two-Factor authentication uses an additional form of verification when you log in. This can improve the security of your email by 99%. It seems obviously worthwhile, and is fairly easy to do.
Your password may not provide much protection. It may have been exposed in the many data breaches, it can be easily attacked, it can be compromised by phishing or keystroke loggers, and it is vulnerable to software bugs. If you grew up using passwords, this may be a bit of an adjustment – passwords just don't work well anymore.

The second form of authentication (2nd factor) can be an email (not recommended); a txt to your phone (less secure); a security app on your phone (good); or a physical device that provides a code that changes every minute (best). You can also use a biometric second factor such as fingerprint or facial recognition with some programs.
Commonly used phone apps: Microsoft Authenticator Google Authenticator Duo Authenticator. Authy can be used from a phone or desktop. We recommend the YubiKey for hardware as a second form of authentication. More 2FA options from PC magazine.

Articles from PC magazine and The Verge on setting up Two-Factor Authentication for commonly used websites.

3. **Avoid Webmail.**

Webmail is accessible from anywhere. It makes it easy for your workers to access their email. It also makes it easy for criminals to access your email system. Webmail adds the risks of web browsing to the email experience. Office 365 allows you to block the use of Webmail, greatly increasing the security of your email system. Outlook with Office 365 can also block access from locations that employees could never be logging in from (such as Russia or China).

Do not allow your employees to access their personal webmail from work computers, including those working from home. This opens an entirely new set of risks.

Avoid older email programs – These often use ways of connecting to the email server that are less secure. Two-Factor Authentication can mitigate this risk but assume there is a good chance of your password being compromised. Some older email programs will automatically connect to any web links in your email when you open the message, potentially installing malware.

4. **Separate work email.**

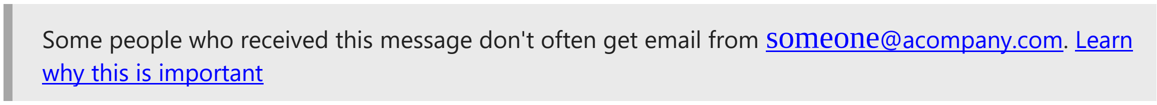
Keep your business email address separate from the email you use to log in to shopping websites, sign up for newsletters, etc. Create separate email addresses for email uses that may be risky. Data breaches will be less likely to impact your business email account, and you won’t be as easily targeted with spam and phishing email.

5. **Enable advanced email protection.**

If you have completed the steps above, the next step is to take advantage of your email provider’s email security features. We recommend Office 365 in part because they are considered a leader in email security.
Microsoft provides some advanced email protection features as part of their Microsoft Defender for Office 365 product. This is well worth the additional cost to protect email accounts for sensitive users such as business owners, accountants, and those in the financial industry.

Once enabled, it provides the following:
Enhanced protection from phishing, spam, and malware.
Safe links: Testing of weblinks before downloading the email.
Safe attachments: Testing of email attachments prior to download.
Provide additional checks to prevent malicious email that appears to be sent from within your company. These messages can appear to be from your boss, perhaps urging you to wire money immediately.

Office 365 users should turn on the following:
Enable additional security checks that validate email by checking the sender’s email settings to see if they are legitimate (SPF, DKIM, and DMARC).
Add a message identifying email coming from outside the organization such as this:
CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
Add a message which warns you if an email is not from someone you normally get email from:



Some people who received this message don't often get email from someone@acompany.com. Learn why this is important

The Microsoft Defender for Identity product provides enhanced protection for user accounts. It uses constantly updated threat data gathered from their security staff, along with AI to detect unusual activity. This includes the following:
Detection of risky sign-in activity, such as logins involving impossible travel.
Detection of suspicious account activity. This warns of actions granting unusual permissions or access, changes in the account security settings, etc. It also provides detailed logging of all user activity, making it possible to track a potential security incident.

In addition, there are some security settings we recommend for anyone using Office 365 which we can review – just ask.

This Video provides a good overview of how these products work to protect your email. It’s about 11 minutes long and well worth your time if you are interested in better security.

Security measures work together to protect your data. Have a good firewall properly configured, keep your software up to date, provide malware protection (anti-virus), and monitor your network to prevent or detect problems.

Tim Torian has his degree in Computer Science and has been consulting on technology for business for the past 30+ Years. He has multiple industry certifications including Microsoft and Cisco. He has taught computer networking at the College of Sequoias and Cal Poly Extension. He was awarded “Entrepreneur of the year” by the Tulare County EDC in 2008. Torian Group was awarded “Technology Business of the Year” by the SBDC in 2011. He is president of Torian Group, Inc. which provides a full range of Technology Consulting services to local business, including computer services, networking, and network design. www.toriangroup.com